Notice of Allowability	**Application No.** 09/666,519	**Applicant(s)** DICKINSON ET AL.	
	Examiner LEYNNA T. HA	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 8/4/2006.

2. ☒ The allowed claim(s) is/are 2, 5-10, 14, 16-29, 36, 59-69 and 75-76.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) ☐ All b) ☐ Some* c) ☐ None of the:

1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

(a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.

(b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

EXAMINER'S AMENDMENT

1. Claims 2, 5-10, 14, 16-29, 32-36, 59-69, and 75-76 have been amended and are allowed over art.

Claims 1, 3-4, 11-13, 15, 30-35, 37-58, and 70-74 have been cancelled by the applicant.

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Don Pelto and Mr. Rob Elliot on 10/23/2006.

3. The following examiner's amendment for claims 1-76 are as follows:

Claim 1: Cancelled.

Claim 2:

A secure cryptographic system, comprising:

a depository system, remote from a user, having at least one server which stores at least one private key and a plurality of enrollment authentication data, wherein each enrollment authentication data identifies one of multiple users;

an authentication engine, remote from said user, which compares authentication data received by from one of said multiple users to enrollment authentication data corresponding to said one of multiple users using at least one private key received from the depository system;

a cryptographic engine which, when the authentication result indicates proper identification of the one of the multiple users, performs cryptographic functions on behalf of the one of the multiple users using the associated one or more different keys received from the depository system; and

a transaction engine connected to route data from the multiple users to the depository server system, said authentication engine, and said cryptographic engine;

wherein said secure cryptographic system is remote from said user and said user is connected to the system via a communication link,

wherein said depository system further comprises a plurality of data storage facilities, each data storage facility having at least one server storing substantially randomized portion of said private key and a substantially randomized portion of said plurality of enrollment authentication data, and

wherein each substantially randomized portion is individually undecipherable.

As per claims 3-4: Cancelled.

As per claim 5: A secure cryptographic system of Claim 2, wherein said enrollment authentication data includes biometric data.

As per claim 6: A secure cryptographic system of Claim 5, wherein said biometric data includes finger print patterns.

As per claim 7: A secure cryptographic system of Claim 2, wherein said at least one private key corresponds to said secure cryptographic system.

As per claim 8: A secure cryptographic system of Claim 2, wherein said at least one private key corresponds to said one of said multiple users.

As per claim 9: A secure cryptographic system of Claim 2, wherein said cryptographic functions comprise one of digital signing, encryption, and decryption.

As per claim 10: A method of facilitating cryptographic functions, said method comprising using the system of claim 2.

As per claims 11-13: Cancelled.

As per claim 14:

An authentication system for uniquely identifying a user through secure storage of the user's enrollment authentication data, said authentication system comprising:

a plurality of data storage facilities, wherein each data storage facility includes a computer accessible storage medium which stores one of substantially randomized data portions of enrollment authentication data from and one of substantially randomized portions of said private key; and

an authentication engine which communicates with said plurality of data storage facilities and comprises

a data splitting module which operates on the enrollment authentication data and said private key to create said substantially randomized data portions;

a data assembling module which processes said substantially randomized data the portions from at least two of the data storage facilities to assemble enrollment authorization data and said private key, and

data comparator module which receives current authentication data from a user and compares the current authentication data with the assembled enrollment authentication data to determine whether said user has been uniquely identified;

wherein said trust engine comprises an authentication system,

wherein said trust engine is remote from said user and said user is connected to said trust engine via a communication link, and wherein each substantially randomized portion is individually undecipherable.

As per claim 15: Cancelled.

As per claim 16: The authentication system of Claim 14, wherein said each data storage facility is logically separated from any other data storage facility.

As per claim 17: The authentication system of Claim 14, wherein said each data storage facility is physically separated from any other data storage facility.

As per claim 18: The authentication system of Claim 14, further comprising a cryptographic engine which, upon the unique identification of said user by said authentication engine, provides cryptographic functionality to said user.

As per claim 19: The authentication system of Claim 14, wherein said plurality of data storage facilities comprises at least one secure server.

As per claim 20: The authentication system of Claim 14, wherein unique identification of said user by said authentication engine provides said user authorization to gain access to or operate one or more systems.

As per claim 21: The authentication system of Claim 20, wherein said one or more systems include one or more electronic devices.

As per claim 22: The authentication system of Claim 20, wherein said one or more systems include one or more computer software systems.

As per claim 23: The authentication system of Claim 20, wherein said one or more systems include one or more consumer electronic.

As per claim 24: The authentication system of Claim 23, wherein said one or more consumer electronics includes a cellular phone.

As per claim 25: The authentication system of Claim 20, wherein said one or more systems include one or more cryptographic systems.

As per claim 26: The authentication system of Claim 20, wherein said one or more systems include one or more physical locations.

As per claim 27: The authentication system of Claim 14, wherein at least one of the data storage facilities stores at least some sensitive data, wherein said at least one of said data storage facilities serves said sensitive data when said authentication engine indicates that said user has been uniquely identified.

As per claim 28: The authentication system of Claim 14, further comprising a data vault which stores sensitive data, wherein said data vault serves said sensitive data when said authentication engine indicates that said user has been uniquely identified.

As per claim 29: The authentication system of Claim 14, wherein said identification system outputs an indication of whether said user has been uniquely identified.

As per claims 30-35: Cancelled.

As per claim 36: A method comprising using the system of claim 14.

As per claims 37-58: Cancelled.

As per claim 59:

A secure authentication system, on a remote trust engine, comprising:

a depository system, remote from a user, having at least one server which stores at least one private key and a plurality of enrollment authentication data, wherein each enrollment authentication data identifies one of multiple user, wherein said depository system further comprises a plurality of data storage facilities, each data storage facility having at least one server storing a substantially randomized portion of said private key and a substantially randomized portion of said plurality of enrollment authentication data;

a plurality of authentication engines, wherein each authentication engine a data assembling module which assembles said substantially randomized enrollment authentication data portions from said depository system to form the enrollment authentication data which uniquely identifies a user to a degree of certainty,

wherein each authentication engine receives current authentication data to compare to said enrollment authentication data, and wherein each authentication engine generates an authentication result; and a redundancy system which receives said authentication result of at least two of the authentication engines and uses said authentication results to determine whether said user has been uniquely identified,

wherein the secure authentication system is part of said remote trust engine;

wherein said remote trust engine is remote from said user and said user is connected to said trust engine via a communication link; and

wherein each substantially randomized portion is individually undecipherable.

As per claim 60: The secure authentication system of Claim 59, wherein said redundancy system determines whether said user has been identified by following the majority of said authentication results.

As per claim 61: The secure authentication system of Claim 59, said redundancy system determines whether said user is uniquely identified by requiring said authentication results to be unanimously positive before issuing a positive identification.

As per claim 62: The secure authentication system of Claim 59, wherein said redundancy system includes a plurality of redundancy modules, and said secure authentication system further comprises:

plurality of geographically remote trust engines, each trust engine having one of said plurality of authentication engines and one of said redundancy modules, wherein the redundancy module for at least one of said plurality of trust engines determines whether said user has been uniquely identified using said authentication results from ones of said authentication engines associated with the other trust engines and without using said authentication results from the at least one trust engine.

As per claim 63: The secure authentication system of Claim 62, wherein said each of the plurality of trust engines includes a depository having a computer accessible storage medium which stores a substantially randomized portion of the enrollment authentication data and wherein each depository forwards the substantially randomized portion of the enrollment authentication data to the plurality of authentication engines.

As per claim 64: The secure authentication system of Claim 62, wherein said determining whether the user has been uniquely identified corresponds to the one of the redundancy modules to first determine a result.

As per claim 65:

A trust engine system for facilitating authentication of a user, said trust engine system comprising:

a first trust engine comprising a first depository, remote from a user, wherein said first depository includes a plurality of data storage facilities, each data storage facility having at least one server storing a substantially randomized portion of at least one piece of enrollment authentication data from a plurality of enrollment authentication data corresponding to multiple users and at least one piece of said private key;

a second trust engine located at a different geographic location than said first trust engine and comprising a second depository having a plurality of data storage facilities, each data storage facility having at least one server storing substantially randomized portion of at least one piece of said enrollment authentication data and at least one piece of said private key;

an authentication engine communicating with the first and second depositories and which assembles at least two of said substantially randomized data portions of at least one piece of said enrollment authentication data and at least one piece of said private key into a usable form, and

an transaction engine communicating with the first and second depositories and the authentication engine,

wherein when said second trust engine is determined to be available to execute a transaction, said transaction engine receives enrollment authentication data from a user and forwards a request for a data assembling module to assemble said enrollment authentication data from substantially randomized data portions using said private key, and wherein the authentication engine compares said authentication data from said user and enrollment authentication data assembled from said first and second depositories, and determines an authentication result,

wherein said first and second trust engines are remote from said user and said user is connected to said trust engines via a communication link; and

wherein each substantially randomized portion is individually undecipherable.

As per claim 66: The trust engine system of Claim 65, wherein said determination of whether said second trust engine is available to execute said transaction includes a determination of whether said second trust engine is within geographic proximity to the user.

As per claim 67: The trust engine system of Claim 65, wherein said determination of whether said determining of whether said second trust engine is available to execute said transaction includes a determination of whether said second trust engine is currently servicing a light system load.

As per claim 68: The trust engine system of Claim 65, wherein said determination of whether said second trust engine is available to execute said transaction includes a determination of whether said second trust engine is currently scheduled for maintenance.

As per claim 69: The trust engine system of Claim 65, wherein said determination of whether said the first and second trust engines are determined to be available, and an authentication result for said trust engine system follows the first and second trust engines to produce the authentication result.

As per claims 70-74: cancelled

As per claim 75: A method comprising using the system of claim 59.

As per claim 76: A method comprising using the system of claim 65.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is

(571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100